Cybersecurity
Progress. Protected.

Reduce uncertainty and accelerate decisions with IOC lookup and sample analysis

5 minutes
validate against the latest ESET data

20 feeds
unique IOCs spanning 20 specialized feeds

900+ in-house experts
intelligence based on the expertise of ESET TI analysts, malware researchers and AI scientists

The problem

Security teams regularly encounter suspicious files and indicators but deciding what to do next isn't always straightforward. Tools may return conflicting verdicts or lack the context needed to explain why something is flagged. **Analysts need clearer, more reliable evidence to reduce uncertainty** without exposing sensitive samples or relying on costly private services. At the same time, SOCs must triage large volumes quickly and investigate priority files in depth without adding noise or infrastructure overhead.

The solution

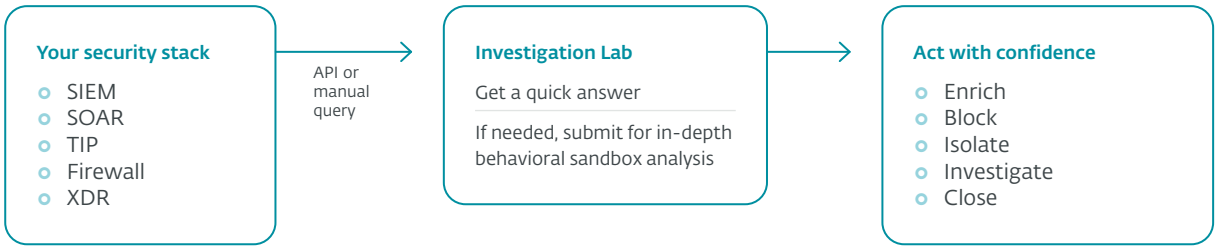
ESET THREAT INTELLIGENCE INVESTIGATION LAB

ESET Threat Intelligence Investigation Lab helps analysts turn suspicious files and indicators into confident decisions. **Get a trusted second opinion** backed by ESET telemetry, reputation data and decades of threat analysis experience, while keeping sensitive investigations private. Use **IOC Search** for quick, low-noise answers at scale, or go deeper with **Sample Submission** when you need richer behavioral evidence and context.

HOW IT WORKS

Investigation Lab: from signal to decision, faster

Investigation Lab integrates through API with the security tools your team already uses. Enrich an alert, decide the next action and submit a sample to the sandbox when deeper behavioral analysis is needed.



WHY IT STANDS OUT

Regional visibility

ESET's global telemetry provides unique visibility into underreported regions, helping deliver trusted answers that may not be available from US-centric sources.

Faster investigation

ESET's decades-built infrastructure, combining global telemetry, AI-driven processing and deep analysis pipelines accelerates investigation and helps you reach actionable answers faster.

Human oversight

AI speeds up analysis, while ESET experts curate and review findings to ensure confirmed indicators are precise, relevant and ready for action.

What's in ESET Threat Intelligence Investigation Lab

	Investigation Lab	Investigation Lab Advanced
Best suited for	Teams needing reliable IOC enrichment and occasional deep file analysis	Teams with higher investigation volumes and advanced analysis needs
Full API Access	Yes	Yes
IoC Search (botnets, C&Cs, domains, IPs, URLs)	1,000/day; 5,000/week	10,000/day; 50,000/week
Advanced querying across ESET database	Yes	Yes
Sample Submission	50/day; 250/week	500/day; 2,500/week
In-depth behavioral analysis	Yes	Yes
Sandbox customization	No	Yes
Sandbox processing priority	Standard	High
Sample privacy	Standard — sample deleted; verdict and hash retained	High — sample, verdict and hash deleted